BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-220
1 MARCH 1997

Communications and Information

ON-HOOK TELEPHONE SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

This instruction discusses the vulnerabilities of administrative telephone systems and outlines responsibilities for on-hook telephone security. It implements AFPD 33-2 and establishes security standards for installing and operating telephone systems in both classified and sensitive discussion areas.

SUMMARY OF REVISIONS

This is the initial publication of AFI 33-220. It substantially revises guidance previously found in AFR 56-14, *Telephone Security*.

1. The Inherent Vulnerability of Administrative Telephone Systems. The administrative telephone system is one of the most common means of communication found in office environments. This includes desk telephones, facsimile machines and computer MODEMs. Their presence in sensitive discussion areas represents a significant threat to technical security.

1.1. The telephone system can provide an unintended electrical path for transmitting information from the area. It may also provide a means for concealing and supplying power to technical surveillance devices. These conditions require commanders to appreciate the inherent vulnerabilities found in telephone equipment and, based on the external threat in the local area, prudently manage the risks posed to their information.

1.2. Administrative telephone system components can also be used to monitor conversations or activities occurring near the telephone system components when the system is on-hook and not in normal use. This makes it extremely difficult for personnel in the facility to be aware that monitoring is occurring. Conversations could be intercepted by exploiting equipment signals, modifying existing equipment or installing surveillance devices which rely on system wiring.

2. Responsibilities.

2.1. Commanders. Commanders responsible for the security of an activity or location where personnel routinely discuss classified or sensitive information, as defined in AFI 33-202, *Computer Security*, or where personnel hold recurring sensitive presentations such as scheduled conferences or briefings, should:

2.1.1. Ensure the number of telephones used is the minimum necessary to meet operational requirements.

2.1.2. Apply appropriate telephone security measures in discussion areas and ensure adequate technical surveillance countermeasures (TSCM) protection as described in Air Force Manual (AFMAN) 33-274, On-Hook Telephone Security Guidelines, is used for all administrative telephones and equipment servicing discussion areas.

2.1.3. Use physical security safeguards to prevent unauthorized personnel from obtaining clandestine physical access to the telephone system or components of the system.

2.2. Air Force Office of Special Investigations (AFOSI). AFOSI is the office of primary responsibility (OPR) for on-hook telephone technical security matters, to include providing guidance for installing and operating telephone systems within the Air Force, and Department of Defense facilities occupied by Air Force affiliated personnel. AFOSI will:

Supersedes: AFR 56-14, 1 April 1991.
OPR: SAF/IGX (Maj Russell W. Merritt)

Certified by: SAF/IG (Col Charles P. Azukas)
Pages: 3/Distribution: F

Please Recycle Printed on Recycled Paper

2.2.1. Provide Air Force representation to the US Government intelligence community's Telephone Security Group (TSG). The TSG is the primary technical and policy resource in the US intelligence community for all aspects of the TSCM program involving telephone systems in areas where sensitive government information is discussed.
2.2.2. Examine the TSCM needs of the Air Force and tailor Air Force telephone security standards to those established by the TSG.
2.2.3. Provide guidance to Air Force organizations on selecting local equipment for installing telephone systems.
2.2.4. Determine the effectiveness and applicability of protective security devices and TSCM procedures for qualified facilities; and, provide information and briefings about the technical threat to telephone systems and the countermeasures intended to nullify that threat. Further information on requesting TSCM services or threat briefings is contained in AFI 71-101, Volume 1, *Criminal Investigations and Counterintelligence*.

RICHARD T. SWOPE, Lt General, USAF
The Inspector General

GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS

References

AFI 71-101, Volume 1, *Criminal Investigations and Counterintelligence*
AFMAN 33-274, *Telephone Security Guidelines*

Abbreviations and Acronyms

AFI−Air Force Instruction
AFMAN−Air Force Manual
AFOSI−Air Force Office of Special Investigations
TSCM−Technical Surveillance Countermeasures
TSG−Telephone Security Group